

**Board of Governors of the Federal Reserve System**

**AUDIT OF THE FEDERAL RESERVE'S  
BACKGROUND INVESTIGATION PROCESS**



---

**OFFICE OF INSPECTOR GENERAL**

---



BOARD OF GOVERNORS  
OF THE  
FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

October 24, 2001

The Honorable Roger W. Ferguson, Jr.  
Vice Chairman and Administrative Governor  
Board of Governors of the Federal Reserve System  
Washington, DC 20551

Dear Vice Chairman Ferguson:

We are pleased to present our *Report on the Audit of the Federal Reserve's Background Investigation Process* (A0107). We performed this audit pursuant to a request from the U.S. House of Representatives Committee on Financial Services, Subcommittee on Oversight and Investigations (Subcommittee). The Subcommittee is concerned that sensitive and private financial data utilized by federal financial regulatory agencies could be improperly accessed, used, or manipulated. Our specific audit objective, based on the Subcommittee's request, was to evaluate the policies, procedures, and practices under which the Board conducts, adjudicates, and documents background investigations of prospective and current employees and contractor personnel. Because Reserve Bank personnel participating in the Board's delegated supervision and regulation program also have access to financial data, we included them in the scope of our audit.

Overall, we found that the Board's policies for conducting background investigations of employees and contractors need to be strengthened. The Board's current policies governing the employee security program are outdated and have not been communicated to all staff with responsibilities for processing security clearances. We also found that there are no documented policies that establish the Board's security requirements for contractors or contractor employees and that summer interns and temporary employees are not required to undergo a background investigation, even though these individuals may potentially have access to sensitive information.

During the audit, we reviewed personnel files for all current Board employees to verify that evidence of a completed background investigation was on file. We performed a similar review for a judgmental sample of contracts (including all contracts for the Division of Information Technology (IT) and the Division of Banking Supervision and Regulation (BS&R) where contractors had authorized access to Board information systems) and for a judgmental sample of personnel files at two Reserve Banks. Our review showed the following:

- Thirty-six out of 1,667 Board personnel files (2.2 percent) did not contain the certificate from the Office of Personnel Management (OPM) showing that a background investigation was completed. We provided these results to the Board's personnel security specialist who requested additional information from OPM regarding background investigations for these

individuals. OPM's records contained case files for twenty of the thirty-six employees, leaving sixteen employees (less than 1 percent) with no record of a completed background investigation. None of the sixteen, however, occupy national security sensitive positions requiring access to secret or top secret information.

- All of the IT and BS&R contractors we reviewed had either completed or were in the process of completing background investigations. We identified several contractor personnel in other divisions, however, working with sensitive payroll, personnel, and medical information for whom a background investigation had not been completed.
- Six out of 112 files (5.4 percent) at one Reserve Bank and one out of 55 files (1.8 percent) at the other Reserve Bank were missing documentation required by the Banks' internal procedures for conducting background investigations.

Our report contains three recommendations designed to improve the Board's background investigation program. Specifically, we recommend that the Staff Director for Management update and clarify the current policies for employee background investigations, develop guidance for conducting and documenting background investigations for contractors, and develop policies and procedures for conducting background investigations for summer interns, temporary employees, and transferred employees. In his written response to the report, the Staff Director for Management concurred with our recommendations and stated that tasks to implement the recommendations will be incorporated with other security related projects stemming from the recent security survey of the Board performed by the U.S. Secret Service, as well as other projects to address new security threats resulting from the events of September 11, 2001. In addition, the Staff Director stated that the Board has ordered background investigations on the individuals for whom we found investigations were missing during our review of personnel files.

We have provided copies of this report to Board management officials and the report will be added to our publicly available Web site. In addition, a copy will be provided to the Subcommittee chairwoman pursuant to her original request. We will also summarize the report in our next semiannual report to the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Barry R. Snyder".

Barry R. Snyder  
Inspector General

Enclosure

**Board of Governors of the Federal Reserve System**

**AUDIT OF THE FEDERAL RESERVE'S  
BACKGROUND INVESTIGATION PROCESS**



---

**OFFICE OF INSPECTOR GENERAL**

---

# TABLE OF CONTENTS

	Page
BACKGROUND.....	1
OBJECTIVES, SCOPE, AND METHODOLOGY .....	1
FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS .....	5
ANALYSIS OF COMMENTS .....	9
APPENDIXES .....	11
Appendix 1 – Division’s Comments .....	13
Appendix 2 – Principal Contributors to this Report.....	15

# BACKGROUND

Earlier this year, the U.S. House of Representatives Committee on Financial Services, Subcommittee on Oversight and Investigations (Subcommittee) requested that the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) perform a review of the Board's background investigation process. The Subcommittee is concerned that sensitive and private financial data utilized by federal financial regulatory agencies could be improperly accessed, used, or manipulated. The Subcommittee feels that it is critical to the safety and security of the financial services industry, and to consumers' confidence in the industry's ability to protect personal financial data, that Board employees or contractors with actual or potential access to such data meet stringent security conditions. In its request, the Subcommittee asked questions relating to (1) the Board's policies for conducting, adjudicating, and documenting background investigations of prospective and current employees and contractor personnel; (2) the Board's procedures for implementing its policies; and (3) the specific manner in which the Board has implemented its background investigation procedures.

## OBJECTIVES, SCOPE AND METHODOLOGY

We conducted fieldwork from April to September 2001. Our audit objective, based on the Subcommittee's request and the specific questions raised, was to evaluate the policies, procedures, and practices under which the Board conducts, adjudicates, and documents background investigations of prospective and current employees and contractor personnel. To accomplish our objective, we met with Board staff responsible for processing and reviewing background investigation documentation and reviewed policies and procedures, as well as current practices, related to the background investigation process. We also reviewed personnel files for all current Board employees and selected a judgmental sample of supporting files in the Board's Security Office to verify that the evidence of a completed background investigation was on file. In addition, we selected a judgmental sample of contracts, including all contracts for the Division of Information Technology (IT) and the Division of Banking Supervision and Regulation (BS&R) where contractors had authorized access to Board information systems, to determine whether a background investigation had been completed on the contractor or the contractor's employees.

Because Reserve Bank personnel participating in the Board's delegated supervision and regulation program also have access to financial data, we included them in the scope of our audit.<sup>1</sup> We requested each Reserve Bank General Auditor, as our Reserve Bank liaisons, to provide us with a copy of the policies and procedures in place for conducting, adjudicating, and documenting background investigations of Reserve Bank examiners and contractor personnel in the supervision and regulation area. We also requested the General Auditors to provide copies of any recent reports, or portions of any reports, pertaining to work they had performed related to

---

<sup>1</sup> The Board is responsible for the supervision and regulation of certain depository institutions and all bank holding companies (BHCs) and financial holding companies (FHCs). Reserve Banks participate in the supervision and regulation program under authority delegated from the Board. The primary supervisory activity is the on-site examination of state-chartered member banks and inspections of BHCs and FHCs to determine safety, soundness, and compliance with applicable laws and regulations. Other supervisory activities are also performed by the Reserve Banks in coordination with the Board.

background investigations. In addition, we tested a judgmental sample of two Reserve Banks' personnel files to verify that a background check was completed. Our audit was conducted in accordance with generally accepted government auditing standards.

## **Employee Background Investigations**

### **Overview**

All Board employees are subject to a background investigation when hired and their continued employment is contingent on a satisfactory background investigation result. The background investigation process includes fingerprinting and completing either Office of Personnel Management's (OPM) Standard Form 85P – Questionnaire for Public Trust Positions (SF 85P) or Standard Form 86 – Questionnaire for National Security Positions (SF 86); the specific form required depends on the position's security classification. The Personnel Security Program within the Division of Support Services (SS) has overall responsibility for administering, controlling, and coordinating all personnel security investigations and security clearances for the Board. SS has developed an internal manual covering security operations, which includes the "Regulations Relating to the Employment Security Program of the Board of Governors of the Federal Reserve System" (Regulations). The Regulations outline policies, standards, and procedures relating to the employment security program.

### **Fingerprinting**

Fingerprints are collected for all new employees during initial employee orientation and are sent to OPM for processing. OPM in turn sends the fingerprints to the Federal Bureau of Investigation (FBI); the Board generally receives fingerprint analysis results from the FBI within two days. If the FBI report shows no derogatory information or issues, the report is filed pending completion of the background investigation process. If the FBI report does contain derogatory information or issues, the report is reviewed by the Director of SS (who serves as the Board's Security Officer) to determine if the employee poses a security risk. In making this determination, the Security Officer considers the seriousness of the issue and the employee's possible access to sensitive information. If the derogatory information or issues are not perceived as security risks, the Security Officer forwards the fingerprint report, together with his evaluation, to the Assistant Director of the Human Resources Function (HR) who reviews the information for a suitability decision. According to the Assistant Director, this review includes the timeframe and nature of the specific issue, the type of work to be performed at the Board, and input from the individual to help put the information in perspective. The Assistant Director works closely with the Board's Legal Division (Legal) and the employee's division director before issuing a final decision regarding the employee's suitability. If the Security Officer believes the employee poses a risk or if an adverse suitability decision is made, the employee is suspended and may be terminated subject to the Board's adjudication process, which is described below.

### **SF 85P and SF 86 Processing**

Individual Board divisions determine the level of security classification for their employees based on the information access and business requirements for the specific position or job family. If the new employee occupies a public trust position, the employee completes a SF 85P.<sup>2</sup> The SF 85P requests information regarding citizenship, prior residences, education, employment, references, marital status, relatives, military record, drug use, police and investigative record, and the employee's financial history. A personnel security specialist in SS reviews the SF 85P for completeness and mails it to OPM along with the Board's Employment Application Form for processing. OPM performs the background investigation and sends a report back to the Board's personnel security specialist. According to the personnel security specialist, OPM reports are generally received within two months. If the OPM investigative report contains derogatory information, the same process as outlined above for fingerprint results is followed. If the OPM investigative report does not contain derogatory information, the personnel security specialist certifies that the investigation has been completed and sends the certification to HR to be filed in the employee's personnel file; the OPM report is filed in the Security Office. Once a new employee completes this process, a periodic reinvestigation is not performed and the employee will only be subject to another background investigation if he or she transfers into a position requiring a higher-level security clearance.

If a division determines that an employee requires either a national security critical sensitive clearance (for access to top-secret information) or a non-critical sensitive clearance (for access to secret information), the division provides the employee's name and appropriate clearance level to the personnel security specialist who provides the employee a SF 86. The SF 86 requests information similar to the SF 85P, although the information requested is generally more detailed. The SF 86 also requests information on the employee's associates, alcohol use, and financial delinquencies. Once the employee completes the SF 86, the personnel security specialist reviews the form for completeness, indicates the level of clearance requested, and sends the form to OPM for processing. When OPM returns the completed background investigation, the Board's Security Officer reviews the report and, if there are no derogatory comments or issues, the security clearance is granted. If there are derogatory comments or issues in the OPM report, the Security Officer, Legal, and the employee's division director will discuss the comments to determine if the security clearance should be granted or sent to the Board for final determination. (See discussion of the adjudication process below.) If the clearance is granted, the OPM report is filed in the Security Office and a certification is forwarded to HR to be included in the employee's personnel file.

When the Security Officer grants the clearance, the personnel security specialist explains to the employee that the employee is authorized access to classified material up to their clearance level to the extent required in the performance of their official duties. The personnel security specialist also provides the employee with a copy of the Board's procedures for handling classified material and requires the employee to acknowledge receipt of this information by signing a copy of the security clearance letter. In addition, the employee is required to sign the classified information nondisclosure agreement.

---

<sup>2</sup> Public trust positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; and positions involving access to, or operation or control of, financial records, with a significant risk for causing damage or realizing personal gains.



Each critical sensitive (top secret) clearance must be reinvestigated every five years and every non-critical sensitive (secret) clearance must be reinvestigated every ten years. Each year, the personnel security specialist circulates a list of all employees with a critical sensitive or non-critical sensitive clearance to the employee's respective division for verification that the clearances are still required. For those employees whose clearance requires reinvestigation, the specialist provides the employee with the required forms and instructions. In addition, for budget purposes the personnel security specialist requests each division to estimate the number of additional clearances that will be required in the next year.

## **Adjudication Process**

The Board's adjudication process differs for new and permanent employees. If a new employee is suspended as a result of derogatory information in a background investigation, the Board notifies the employee in writing of the reasons for the suspension. The suspended employee has the right to submit, within thirty days after notification, statements and affidavits refuting or explaining the stated reasons for the suspension. The Security Officer and Legal will review the information and make a recommendation to the Board. The Board then makes a final, written determination to either reinstate or terminate the employee.

If the suspension pertains to an employee with a permanent or indefinite appointment who has completed his/her probationary period (e.g., a permanent employee transferring from a public trust position to a national security sensitive position), the Board provides the employee with a written statement that outlines the specific information as to the reasons for suspension. Before issuing the written statement, the Board consults with Department of Justice to ensure that the rights of the employee are fully considered. Within thirty days of notification, the employee has the opportunity to submit statements refuting the basis for the suspension and to provide supporting documents and affidavits. The Security Officer and Legal will review this information and make a recommendation to the Board. If the Board believes there is still a security risk, the employee is given a hearing before a security hearing board composed of at least three impartial, disinterested individuals (civilian officers or employees of the federal government selected by the Board from OPM rosters). The security hearing board's decision will be in writing and submitted to the Board and the suspended employee. The Board will review the entire case before making a final decision and will provide the employee with a written notice of the final decision.

## **Contractor Background Investigations**

Individual Board divisions determine if a contractor or contractor personnel require a background investigation based on the type of work to be performed and whether that work will include access to sensitive information. The process for conducting a background investigation for contractors generally follows the procedure for new employees; i.e., the contractor's employees are fingerprinted and, if required by the division, complete a SF 85P.<sup>3</sup> If either report contains derogatory information or issues, the Security Officer will discuss the information with

---

<sup>3</sup> The Board is not authorized to issue clearances to contractor personnel for national security sensitive positions.

the division director responsible for the contract to determine if the contractor's employee should be replaced. Generally, the contractor or its employees will have a chance to refute any of the comments made in either report before a final decision is made.

## **Reserve Bank Background Investigations**

Each Reserve Bank develops and maintains its own policies and procedures addressing background investigations. All Reserve Banks fingerprint new employees and conduct a background investigation. The fingerprints are collected by Reserve Bank staff and sent to OPM for processing. OPM in turn sends the fingerprints to the FBI. The FBI returns their analysis reports to the Reserve Banks. The background investigation, which is conducted either by Reserve Bank HR staff or private contractors, generally includes verification of scholastic and employment information as well as the employee's citizenship or legal authorization to work in the United States. In addition, ten of the twelve Reserve Banks complete a credit check as part of their investigative processes. The Reserve Banks have also established their own adjudication processes, which generally involves a review of derogatory information by the Bank's HR department and senior management. Contractor personnel in the Reserve Banks' supervision and regulation areas are generally subject to the same investigative process as Reserve Bank employees, although we found that one Reserve Bank may conduct drug testing on contractor personnel depending on the position.

The Board processes national security critical sensitive and non-critical sensitive clearances for the Federal Reserve Banks. The Board requires that each Federal Reserve President and First Vice President have critical sensitive (top secret) clearances, as they may encounter national security classified information at that level while performing their official duties. Each Reserve Bank is responsible for identifying other individuals that may have a business need for national security information while performing their official duties. Processing a SF 86 for Reserve Bank employees is the same as for Board employees except that the Board's Security Officer discusses any derogatory information or issues with the Reserve Bank's President and First Vice President before a decision is made to grant or deny the clearance. According to the Board's Security Officer, the Reserve Banks follow the same adjudication process for national security sensitive positions as for their other background investigations.

## **FINDINGS, CONCLUSIONS AND RECOMMENDATIONS**

Overall, we found that the Board's policies for conducting background investigations of employees and contractors need to be strengthened. The Board's current policies governing the employee security program are outdated and have not been communicated to all staff with responsibilities for processing security clearances. We also found that there are no documented policies that establish the Board's security requirements for contractors or contractor employees. Our review identified several contractor personnel working with sensitive personnel information for whom a background investigation had not been completed. In addition, we found that summer interns and temporary employees are not required to undergo a background

investigation, even though these individuals may potentially have access to sensitive information.

Although the procedures for conducting and documenting the investigative process were generally sufficient, our review of personnel files for all current Board employees showed that thirty-six out of 1,667 files (2.2 percent) did not contain the OPM certificate showing that a background investigation was completed. We provided these results to the personnel security specialist who checked the security files and then requested additional information from OPM regarding background investigations for these individuals. OPM's records contained case files for twenty of the thirty-six employees in question, leaving sixteen employees (less than 1 percent) with no record of a completed background investigation. The sixteen positions included consumer and information technology analysts, administration and maintenance staff, economist and senior economists, and managers. None of the sixteen occupy national security sensitive positions and three are no longer employed by the Board. Of the remaining thirteen, three are employees who either transferred from another agency or moved from summer intern or temporary positions to permanent employment. One currently occupies a part-time position and one is currently completing the SF 85P even though this employee has been employed by the Board since 1998. As for the remaining eight positions, three employees believe they completed the background investigation form; however, the remaining five could not recall doing this.

Our review of a judgmental sample of seventy-eight security files (sixty-nine involving national security sensitive positions and nine involving public trust positions) showed that all documentation supporting the certificates had been completed and was on file. During our review, we did not identify any issues regarding the timeliness or effectiveness of the Board's adjudication process.

We also found the Reserve Banks' internal procedures for reviewing the backgrounds of supervision and regulation personnel were generally effective, although at one of the two Reserve Banks, where we performed additional review of personnel files, we found that six out of 112 files judgmentally selected (5.4 percent) were missing one of the background requirements (that is, missing the fingerprint results or the credit check information). At the other Reserve Bank, we found that one out of fifty-five files judgmentally selected (1.8 percent) was missing one of the requirements. In neither sample, however, did we find the complete background investigation documentation missing. Procedures provided by the Reserve Banks also showed that contractors in the supervision and regulation area complete similar background investigations; however, neither of the Reserve Banks we visited had any contractors presently working in this area.

Our report contains three recommendations designed to improve the Board's background investigation program.

- 1. We recommend that the Staff Director for Management update and clarify the current policies for employee background investigations and include the revised guidance in the *Internal Administrative Procedures Manual* (IAPM).**

The Regulations were most recently revised in September 1984. Although the Regulations generally follow the Board's current procedures for completing background investigations, they are incomplete and outdated in several areas. For example, the Regulations do not provide

sufficient guidance for determining the specific positions or job families that require a security clearance. The Regulations provide general guidance regarding positions with access to national security information, positions involved in policy-making, and positions involving fiduciary duties. There is no guidance, however, regarding Board requirements or expectations for the clearances required for the specific types of positions supporting the Board's primary mission areas or the specific risks that the Board considers relevant in reaching a security or suitability decision. In addition, the Regulations are silent regarding the requirements for Reserve Bank personnel, even though the Board processes the national security clearances for the Reserve Banks.

The Regulations also do not clearly define all participants' responsibilities in the background investigation process. For example, the Board has designated a "Suitability Officer" with the responsibility to review derogatory information or issues for a suitability decision after the Security Officer has made the security decision. However, the "Suitability Officer" is not mentioned in the Regulations. Instead, the Regulations imply that the Security Officer and the Board are responsible for making both the security decision and the suitability decision. The Regulations are also silent regarding the employee's responsibility for timely submission of required documents and the consequences for failing to meet those timeframes. The personnel security specialist told us that failure to promptly complete the required information results in repeated requests for information and can greatly expand the time required to complete the clearance process.

We believe the Staff Director should revise the Regulations to provide clear guidance to all Board and Reserve Bank staff involved with the background investigation process. The guidance should address requirements for determining the type of clearance required for System-specific positions, as well as all related roles and responsibilities in the background investigation process. After the Regulations have been revised, we believe the updated guidance should be included in IAPM. During our audit, we interviewed all of the division administrators since they are generally the divisions' focal point for processing security clearances. None of the division administrators were aware of any Board policy or guidance regarding security clearances; the personnel security specialist was the only individual with whom we spoke who was using the Regulations for guidance. The division administrators rely on the yearly list from the personnel security specialist to review the clearances within their divisions and determine if any new clearances are required or if individuals have transferred to a different position requiring another type of clearance. Publishing the Regulations as part of the IAPM would provide all employees with an understanding of the Board's background investigation requirements, the roles and responsibilities, and the associated processing procedures.

**2. We recommend that the Staff Director for Management develop guidance for conducting and documenting background investigations for contractors.**

The Board has not established requirements or provided guidance for completing background investigations for contractors or contractor personnel. The Regulations only discuss policies and procedures pertaining to background investigations for Board employees. Furthermore, the Board's "Acquisition Policy"—which governs the Board's acquisition of supplies, services, and construction—is silent regarding security requirements for contractors. The personnel security specialist told us that each Board division or office has the responsibility to identify contractors

requiring a background investigation. In our discussion with division administrators, however, we found that most were under the impression that the Management Division's Procurement Section would determine whether background investigations were required.

We reviewed a judgmental sample of security files pertaining to thirty contracts to determine whether a background investigation had been completed. Our sample included contractors that may have regular access to Board premises or potentially have access to sensitive information, including access to the Board's computer network. Our analysis showed that out of twenty-two contractors from IT, eighteen had a completed background investigation on file and four were in the process of completing the investigative process. Of the two BS&R contracts we reviewed, one background investigation was completed and one was in process. Our review did identify, however, several contractor personnel working in the Management Division with access to sensitive information for whom a background investigation had not been completed. For example, we found two contractor employees working on the Board's payroll and personnel system that did not have a background investigation. We also found that a contract nurse (with access to employee medical records) and a benefits counselor (with access to personnel information) did not have a background investigation.

We believe the Staff Director should provide guidance that establishes a general framework under which divisions determine the specific need for background investigations of contractor personnel. For example, background investigations could be required for any contractor with potential access to certain categories of information, including salary and personnel data or banking supervisory or regulatory information. The guidance could also require that any contractor with access to the Board's premises or the computer network undergo a background investigation. The Staff Director should also clearly define roles and responsibilities for all parties in the contracting process, including the security staff, the procurement staff, and the divisions requiring the specific contractual service. Once developed, the guidance should be incorporated into procedures that are clearly communicated to all responsible individuals. The guidance could, for example, be included in the IAPM either as part of the revised Regulations, as part of the "Acquisition Policy", or as a separate policy and procedures document.

**3. We recommend that the Staff Director for Management develop policies and procedures for conducting background investigations for summer interns, temporary employees, and transferred employees.**

The Board hires summer interns and temporary employees to help support its internal operations. HR handles the hiring process for these employees. Summer intern applicants are required to submit an application, a resume, three references, and school transcripts; successful candidates work from approximately June 1 to September 1. Temporary workers are required to submit an application, a resume, and school transcripts; their duration of employment varies, depending on the nature of the assignment. Summer interns and temporary employees receive a Board identification badge that allows them full access to the Board's buildings and some could have access to sensitive banking and financial data. HR informed us that due to the short term of these assignments, a full background investigation is not performed. In addition, summer interns and temporary employees are fingerprinted only if the division requires it or if the temporary employee's assignment is greater than three months.

Because interns and temporary employees could come in contact with sensitive information, we believe some level of background investigation should be performed. At a minimum, all interns and temporary employees should be fingerprinted. Procedures should also be developed to ensure that summer interns and temporary employees undergo a complete background investigation prior to obtaining permanent employment. At least two of the files in our sample for which background investigation documentation was missing included interns and temporary employees who had transferred to permanent positions. Since these employees already have records in the Board's personnel system, the requirement to complete the background investigation process prior to their change in employment status may be overlooked.

The Staff Director also needs to develop policies and procedures clarifying the requirements when employees transfer within the Board. Employees are eligible to transfer from one position to another generally after six months of employment. When this occurs, the gaining division is responsible for verifying that the transferring employee possesses the required security clearance level for the new position. However, there are no written procedures for implementing this process. We found that when an employee transfers to a different division or the employee's official duties change and a lower level of security clearance is required, security files related to the previous position are destroyed after two years. When this occurs, there is no record on file that a background investigation was ever performed for that employee. We believe the policy should require retention of this information until the employee is no longer working for the Board.

## **ANALYSIS OF COMMENTS**

We provided a copy of this report to the Staff Director for Management for review and comment. His response is included as appendix 1 to this report. The Staff Director's response concurs with our recommendations and indicates that a Board officer has been assigned responsibility to oversee the recommendations' implementation. In his response, the Staff Director also states that tasks to implement the recommendations will be incorporated with other security related projects stemming from the recent security survey of the Board performed by the U.S. Secret Service as well as other projects to address new security threats resulting from recent national events. In addition, the Board has ordered background investigations on the thirteen individuals for whom we found investigations were missing during our review of personnel files for all current Board employees.

## **APPENDIXES**

## Appendix 1 - Division's Comments



**BOARD OF GOVERNORS  
OF THE  
FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551**

**STEPHEN R. MALPHRUS  
STAFF DIRECTOR FOR MANAGEMENT**

DATE: October 17, 2001  
To: Barry Snyder  
FROM: Steve Malphrus *SRU*  
SUBJECT: Response to Audit Recommendation

We appreciate the opportunity to respond to the recommendations provided in the *Audit of the Federal Reserve's Background Investigation Process*. As indicated in our response (attached), we generally concur with the recommendations. Tasks to implement the recommendations will be incorporated with the other security related projects stemming from the recent report from the United States Secret Service (USSS) (last summer we asked the USSS to perform a security survey) as well as other projects to address new security threats resulting from the September 11 terrorist incidents. There are a number of overlaps among the three and the projects will be managed as a rational and interrelated set of work. I have designated Chris Fields as the officer responsible to oversee the Board's work to implement the audit recommendations. Chris will work with Dave Williams, Darrell Pauley, Steve Clark, and Will Cooper.

We commend you and your staff for the collaborative approach to this audit. Please contact me if you have questions or comments.

### Attachment

c: Darrell Pauley  
Dave Williams  
Steve Clark  
Steve Siciliano  
Chris Fields  
Will Cooper



## Appendix 1 - Division's Comments



BOARD OF GOVERNORS  
OF THE  
FEDERAL RESERVE SYSTEM  
WASHINGTON, D. C. 20551

STEPHEN R. MALPHRUS  
STAFF DIRECTOR FOR MANAGEMENT

DATE: October 17, 2001  
To: Barry Snyder  
FROM: Steve Malphrus *SM*  
SUBJECT: Response to Audit Recommendation

We appreciate the opportunity to respond to the recommendations provided in the *Audit of the Federal Reserve's Background Investigation Process*. As indicated in our response (attached), we generally concur with the recommendations. Tasks to implement the recommendations will be incorporated with the other security related projects stemming from the recent report from the United States Secret Service (USSS) (last summer we asked the USSS to perform a security survey) as well as other projects to address new security threats resulting from the September 11 terrorist incidents. There are a number of overlaps among the three and the projects will be managed as a rational and interrelated set of work. I have designated Chris Fields as the officer responsible to oversee the Board's work to implement the audit recommendations. Chris will work with Dave Williams, Darrell Pauley, Steve Clark, and Will Cooper.

We commend you and your staff for the collaborative approach to this audit. Please contact me if you have questions or comments.

Attachment

c: Darrell Pauley  
Dave Williams  
Steve Clark  
Steve Siciliano  
Chris Fields  
Will Cooper

## Appendix 1 - Division's Comments (con't)

### Responses to Recommendations Contained in the *Audit of the Federal Reserve's Background Investigation Process*

1. We recommend that the Staff Director for Management update and clarify the current policies for employee background investigations and include the revised guidance in the *Internal Administrative Procedures Manual (IAPM)*.

Concur. Staff from the Support Services and Management divisions, with assistance from the Legal Division, will clarify and revise the policy regarding employee background investigations to provide clear guidance to all Board staff involved with the background investigation process. Guidance will also clarify the process for determining the specific positions or job families that are designated as "public trust" and "national security" positions.

Background investigations have been ordered for the thirteen individuals for whom investigations were found to be missing or incomplete. Steps have been taken to ensure all new employees, regardless of the hiring process, receive the background investigation.

2. We recommend that the Staff Director for Management develop guidance for conducting and documenting background investigations for contractors.

Concur. Background investigations are conducted for services contracted out on a long-term basis including custodial and cafeteria employees. In the past, the Board has not done background checks on temporary employees because of the lag in receiving the results. Some form of investigations for contractors and consultants on short- or immediate-term contacts will be implemented. We have been evaluating alternatives and have formally requested access to the online computer name-check system used to clear visitors to Treasury. Access to this resource would provide the Board with "a real-time" investigative capability. Though lagged, we will also continue with the system of submitting new employee fingerprints to the Office of Personnel Management (OPM) as well.

3. We recommend that the Staff Director for Management develop policies and procedures for conducting background investigations for summer interns, temporary employees, and transferred employees.

Concur. As discussed in item two, if granted access to the name-check system, the Board will clear all interns and temporary and transferred employees. The OPM fingerprint check will also be made; and when appropriate, the Standard Form 85P, Questionnaire for Public Trust Positions, will be conducted.

## **Appendix 2 - Principal Contributors to This Report**

Mike Green, Senior Auditor and Auditor-in-Charge

Silvia Vizcarra, Auditor

Bill Mitchell, Program Manager